(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 December 2000 (21.12.2000)

PCT

(10) International Publication Number
WO 00/78070 A1

(51) International Patent Classification[7]: H04Q 7/22, 7/32

(21) International Application Number: PCT/SE00/01169

(22) International Filing Date: 6 June 2000 (06.06.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
19992839 10 June 1999 (10.06.1999) NO

(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors: KIESSLING, Johan; Rödabergsbrinken 16, S-113 30 Stockholm (SE). VAN DO, Than; Stjernemyrveien 28, N-0673 Oslo (NO).

(74) Agent: NORIN, Klas; Ericsson Radio Systems AB, Common Patent Department, S-164 80 Stockholm (SE).

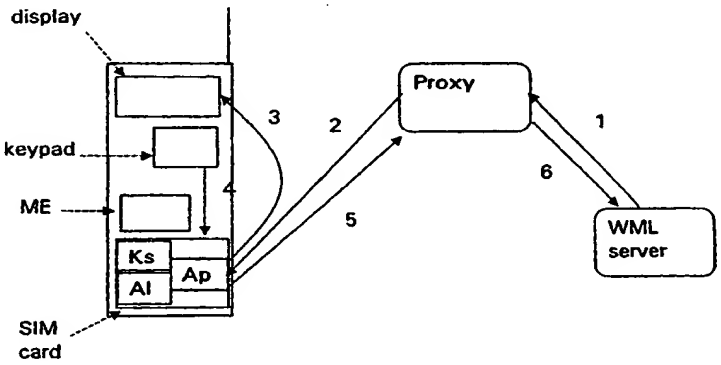
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SAT BACK CHANNEL SECURITY SOLUTION FOR MOBILE TERMINALS USING USSD



MS: Mobile Station
ME: Mobile Equipment
WML: Wireless Markup Language
Ks: Secret/Private Key
AI: symmetric /assymmetric Cryptographic algorithm
Ap: SAT application

(57) Abstract: The present invention relates to a method and an arrangement for performing secure transactions during an information dialogue between a mobile terminal and a WAP server in a mobile network. The dialogue is made by using USSD. According to the invention there is provided a SAT application on the SIM card of the terminal that signs and encrypts data which are to be transferred in a secure way.

WO 00/78070 A1

SAT BACK CHANNEL SECURITY SOLUTION FOR MOBILE TERMINALS USING USSD

The present invention relates to mobile communication, in particular security solutions for mobile terminals using USSD (Unstructured Supplementary Service Data).

BACKGROUND

For mobile terminals not supporting WAP, e.g. most mobile phones at the moment, there exist the possibility of viewing WAP pages through USSD. In other words, a simulation of a WAP (Wireless Application Protocol) information dialogue can be made by using the USSD capabilities of a Mobile Terminal. The WAP WML (Wireless Markup Language) is browsed in a proxy in the network, and the display of the terminal is made for showing the correct message by sending the equivalent of a "screen dump". WML responses are put together by the proxy from the characters entered by the user on the keypad of the Mobile Terminal. This is summarised in Figure 1 as follows:

1. The WML server sends the content of a WML page to the Proxy

2. The Proxy decomposes the WML page onto USSD (Unstructured Supplementary Service Data) and sends the data to the ME (Mobile Equipment)

3. The ME sends the received data to the display, which presents said data to the user

4. If an answer from the user is requested, then the user can enter it to the keypad, which forwards the answer to the ME

5. The ME sends the input to the proxy

6. The proxy assembles the received input into WML format and delivers it to the WML server

No security feature except for unencrypted passwords is available in this solution. It is not possible to have a secure transaction, i.e. encrypted message exchange in this architecture.

State of the art

As mentioned above, the only security feature that exists is the unencrypted passwords. This security feature is implemented in the SAT applications, which implement the information browsing.

Problem

The problem with USSD based browsing as described above, is that the level of security is too low for higher values. As the password is communicated unencrypted, it can be discovered during the transfer. Another problem is that the system is awkward in use. Each time a secure transaction is to be performed, the WML server prompts the user for a password, which password has to be entered manually. The password has to be remembered by the user, possibly in addition to a number of passwords for other applications.

The invention

It is therefore an object of the present invention to provide a method for USSD based browsing, which allows transactions to be performed at a security level hitherto unknown. It is another object of the present invention that said transactions should be easy to perform from the users point of view, and if desired, made fully transparent to the user.

These objects are satisfied in a method as specified in the appended patent claims.

The drawings

Figure 1 illustrates the simulation of a WAP information dialogue using USSD (prior art).

Figure 2 illustrates a secure WAP exchange according to the invention using an SAT back channel.

Description of the inventive solution

For SAT (SIM Application Toolkit (ETSI 11.14)) enabled phones, the following solution is suggested.

As shown in Figure 2, a secret/private key is stored on the SIM card. Also an algorithm for signing data using a symmetric or an asymmetric technique, as well as an application handling the dialogue with the user and the signing of data is stored on the SIM card.

1. When information browsing through the mechanism described above and in Figure 1, has reached a point where a secure transaction should be established, for example the WML server asking explicitly for a secure transaction.

2. The USSD dialogue is terminated. Instead the proxy enters the details of the transaction to be secured into an SMS, and sends it to the SIM card of the Mobile Terminal where the SAT application is activated.

3. The application using SAT commands shows the details of the transaction to the user, and prompts for an "OK" to the transaction.

4. If the user agrees (optionally by entering a PIN), the application signs the data (or a hash of the data) with the secret/private key using the correct algorithms.

5. The signed data is then returned to the proxy by using SMS or USSD as a bearer.

6. Then the proxy either verifies the signature or passes it on to the appropriate instance that shall handle the verification.

Merits of the invention

A very high level of security is achieved in combination with a very flexible information browsing solution.

Since it only has to handle signing of data and no information or menu handling, the application on the SIM card can be made very thin and flexible. Thus, it can be made to work in many different applications.

The system handling the information browsing, and the system handling the security of the transactions are separated. They can be updated, changed etc. independently.

Abbreviations

Application	An application consists of a set of security mechanisms, files, data and protocols (excluding transmission protocols)
ETSI	European Telecommunication Standard Institute
HDML	Hand-held Device Markup Language An abbreviated version of HTML designed to enabling wireless pagers, cellular phones and other hand-held devices to obtain Web pages
HTML	HyperText Markup Language The document format used on the World Wide Web. Web pages are built with HTML tags or codes embedded in the text. HTML defines the page layout, fonts and graphic elements, as well as the hypertext links to other documents on the Web.
PIN	Personal Identification Number
Proxy	It is also called a "proxy server" or "application level gateway". It is an application that breaks the connection between the sender and the receiver. All input is forwarded to a different port, closing a straight path between two networks and preventing a hacker from obtaining internal addresses and details of a private network.
SAT	SIM Application Toolkit SAT is a set of applications and related procedures, which may be used during a GSM session.
SIM	Subscriber Identity Module (Mobile)
SMS	Short Message Service
USSD	Unstructured Supplementary Service Data USSD is a mechanism that allows user interaction between GSM Public Land Mobile Network applications and a Mobile Station in a transparent way through the network.

WAP	Wireless Application Protocol WAP is a wireless standard from Motorola, Ericsson and Nokia for providing mostly cellular phones with access to e-mail and text-based Web pages. WAP uses the Wireless Markup Language (WML), which is the WAP version of HDML.

Patent claims

1. Method for performing a secure transaction during an information dialogue between a mobile terminal and a server in a network,
characterised in that

- said server supporting WML, e.g. a WAP server
- said information dialogue is simulated by using USSD
- the server sends the content of a WML page to a proxy
- the proxy decomposes the WML page onto USSD and sends the data to the mobile terminal
- the mobile terminal sends the received data to the display, which presents said data to the user
- when information browsing has reached a point where a secure transaction should be established, the USSD dialogue is terminated
- the proxy enters the details of the transaction to be secured into an SMS and sends it to the SIM card of the mobile terminal
- a SAT application is activated in the mobile terminal
- the application shows the details of the transaction to the user and prompts for an "OK" to the transaction
- if the user agrees, the application signs the data with a secret/private key
- the signed data is returned to the proxy
- the proxy has the signature verified

- the proxy assembles the signed data into WML format and delivers them to the server.

2. Method according to claim 1, characterised in that said step of agreeing to the transaction involves entering a PIN code.

3. Method according to claim 1 or 2, characterised in that said data is hash coded before signing.

4. Method according to claim 1-3, characterised in that the signed data is returned to the proxy by using SMS as a bearer.

5. Method according to claim 1-3, characterised in that the signed data is returned to the proxy by using USSD as a bearer.

6. Method according to one of the preceding claims, characterised in that the signed data is verified by the proxy.

7. Method according to one of the preceding claims, characterised in that the signed data is passed on to an external instance for verification by the proxy.

8. Arrangement for performing a secure transaction during an information dialogue between a mobile terminal and a server in a network, characterised in that

- said server being a WAP server supporting WML, said information dialogue is simulated by using USSD

- the server is arranged to transfer the content of a WML page to a proxy

- the proxy decomposes the WML page onto USSD and sends the data to the mobile terminal

- the mobile terminal is arranged to present the received data to the user on a display

- said USSD dialogue is terminated when a secure transaction is to be established

- the proxy enters the details of the transaction to be secured into an SMS and sends it to the SIM card of the mobile terminal

- there is installed a SAT application on said SIM card

- said application is arranged to show the details of the transaction for the user and prompt for an "OK" to the transaction

- if the user agrees, the application signs the data with a secret/private key

- the signed data is returned to the proxy

- the proxy has verified the signature

- the proxy assembles the signed data into WML format and delivers it to the server.

9. Arrangement according to claim 8, characterised in that said SAT application is arranged to prompt the user for entering a PIN code.

10. Arrangement according to claim 8 or 9, characterised in that said SAT application is arranged to hash code said data before signing.

11. Arrangement according to claim 8-10, characterised in that the signed data is returned to the proxy by using SMS as a bearer.

12. Arrangement according to claim 8-10, characterised in that the signed data is returned to the proxy by using USSD as a bearer.

13. Arrangement according to one of the claims 8-12, characterised in that the proxy is arranged to verify the signed data.

14. Arrangement according to one of the claims 8-12, characterised in that the proxy is arranged to pass the data to an external instance for verification.

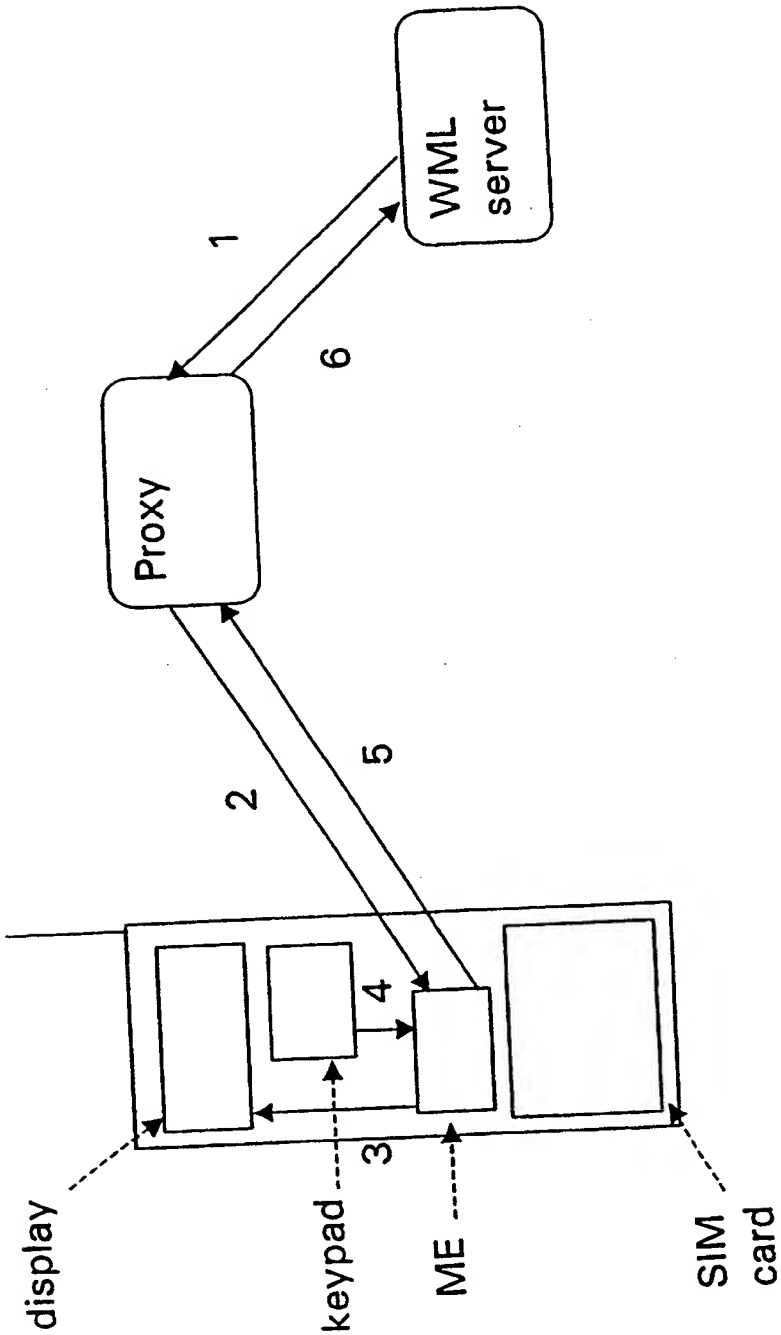
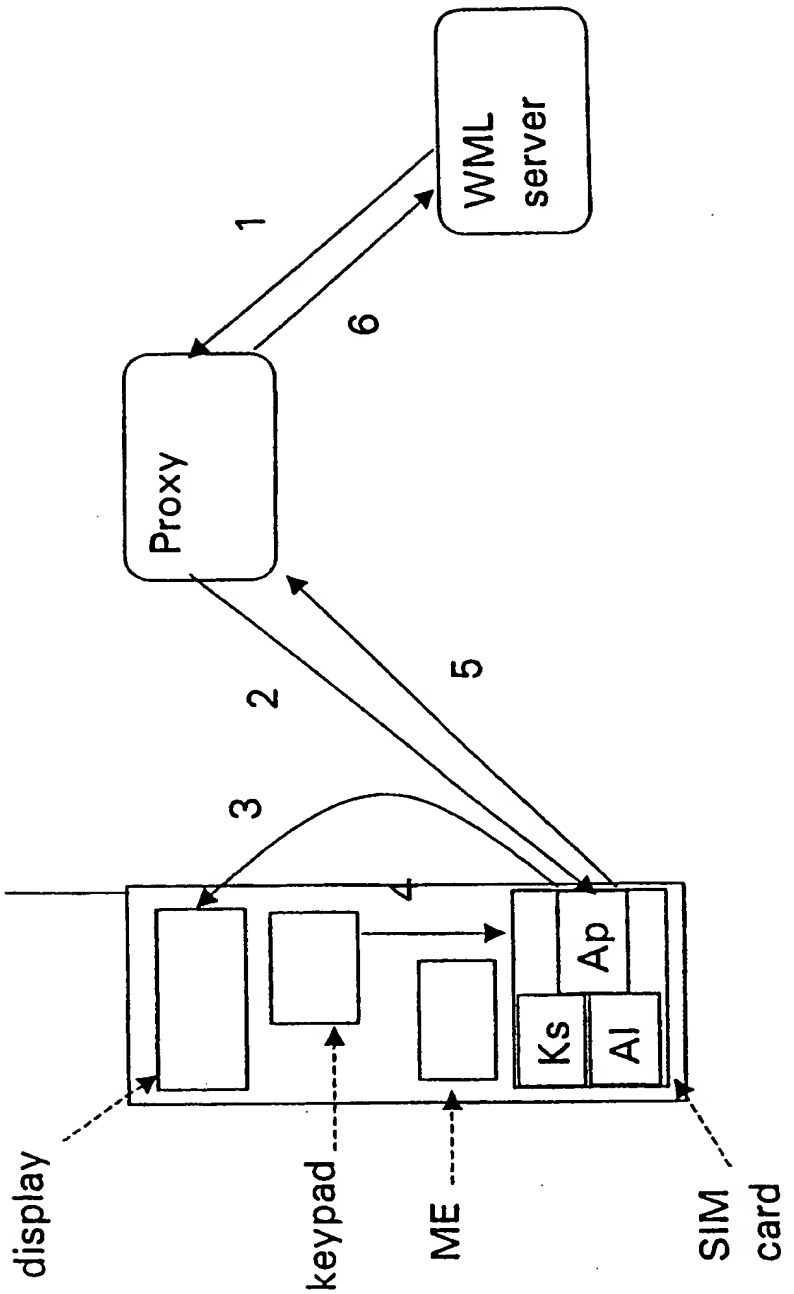

WML server
Proxy
1
2
3
4
5
6
display
keypad
ME
SIM card
MS
MS: Mobile Station
ME: Mobile Equipment
WML: Wireless Markup Language

Figure 1



MS: Mobile Station
ME: Mobile Equipment
WML: Wireless Markup Language
Ks: Secret/Private Key
Al: symmetric /assymmetric Cryptographic algorithm
Ap: SAT application

Figure 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 00/01169

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04Q 7/22, H04Q 7/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	GB 2342817 A (NOKIA MOBILE PHONES LIMITED), 19 April 2000 (19.04.00), page 6, line 23 - page 8, line 2; page 9, line 21 - page 10, line 24; page 13, line 7 - line 29	1-14
Y	WO 9904583 A1 (ORANGE PERSONAL COMMUNICATIONS SERVICES LIMITED), 28 January 1999 (28.01.99), abstract	1-14
A	WAP Architecture Version 30-Apr-1998 Wireless Application Protocol Architecture Specification, page 18, figure 5	1-14

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 August 2000	12 -09- 2000
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Nabil Ayoub / MRo Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 00/01169

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	EP 0989712 A2 (PHONE. COM, INC.), 29 March 2000 (29.03.00), the whole document --	1-14
P,X	WO 9939524 A1 (SONERA OY), 5 August 1999 (05.08.99), page 2, line 34 - page 6, line 9 -- --------	1-14

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2342817 A	19/04/00	GB 9822674 D	00/00/00
WO 9904583 A1	28/01/99	AU 8348798 A	10/02/99
		EP 0997047 A	03/05/00
		GB 2327567 A	27/01/99
		GB 9715097 D	00/00/00
EP 0989712 A2	29/03/00	NONE	
WO 9939524 A1	05/08/99	AU 1970699 A	16/08/99
		FI 3609 U	28/09/98
		FI 980085 D,V	17/02/98
		FI 982129 D	00/00/00